Rule creation

Just my random thoughts, but having to implement something I wonder what is the *best practice for creating rules to mitigate volumetric attacks based on flowspec*?

According to awsstatic.com DDoS attacks are most common at layers 3, 4, 6, and 7 of the Open Systems Interconnection (OSI) model.

Layer 3 and 4 attacks correspond to the Network and Transport layers of the OSI model: these are volumetric infrastructure layer attacks.

Layer 6 and 7 attacks correspond to the Presentation and Application layers of the OSI model, these are as application layer attacks and only the volumetric attacks can be detected by fastnetmon.

#	Layer	Unit	Description	Vector Examples
7	Application	Data	Network process to application	HTTP floods, DNS query floods
6	Presentation	Data	Data representation and encryption	SSL abuse
5	Session	Data	Interhost communication	N/A
4	Transport	Segments	End-to-end connections and reliability	SYN floods
3	Network	Packets	Path determination and logical addressing	UDP reflection attacks
2	Data Link	Frames	Physical addressing	N/A
1	Physical	Bits	Media, signal, and binary transmission	N/A

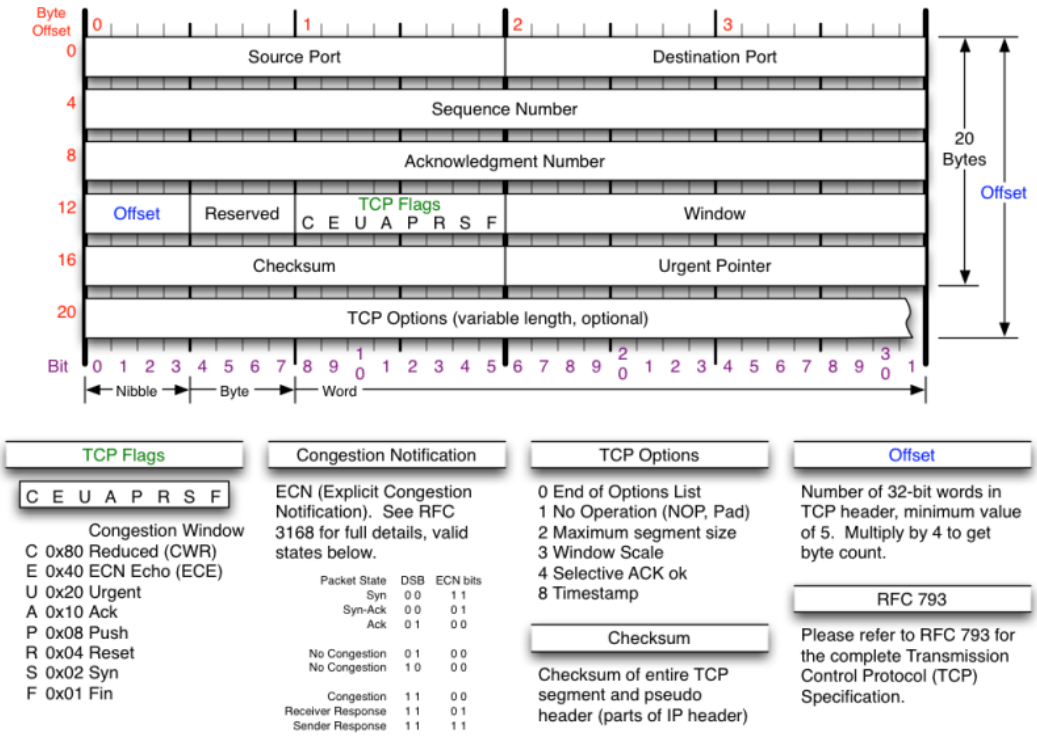
From awsstatic.com

Fastnetmon detects the following type of attacks:

1. *syn_flood*: TCP packets with enabled SYN flag
2. *udp_flood*: flood with UDP packets (so recently in result of amplification)
3. *icmp flood*: flood with ICMP packets
4. *ip_fragmentation_flood*: IP packets with MF flag set or with non zero fragment offset
5. *DNS amplification*:
6. *NTP amplification*:
7. *SSDP amplification*:
8. *SNMP amplification*:

First: it is sometimes possible to distinguish between legitimate and illegitimate packets, as Not All SYNs Are Created Equal . And empty UDP and TCP packet might be rare:

For ethernet is the *minimum payload* 42 octets when an 802.1Q tag is present and 46 octets when absent according to wikipedia on ethernet frames . The minimum Layer 2 Ethernet frame size is 64 bytes for an *empty tcp or udp packet*.



We have the following values for creating a filter:

```
Type 1 - Destination Prefix
Type 2 - Source Prefix
Type 3 - IP Protocol
Type 4 — Source or Destination Port
Type 5 — Destination Port
Type 6 - Source Port
Type 7 — ICMP Type
Type 8 — ICMP Code
Type 9 - TCP flags
Type 10 - Packet length
Type 11 — DSCP
Type 12 - Fragment Encoding
```

Suggestion for rule creation:

Attack type	Mitigation	Match on
syn_flood	rate-limit	tcp option (syn) protocol, destination port, tcp flags, size, (ttl would be nice but is still in draft), and source any
udp_flood	rate-limit	protocol and destination host and port
icmp flood	discard	protocol and destination
ip_fragmentation_flood	rate-limit	protocol and destination
DNS amplification	rate-limit	protocol, port and destination
NTP amplification	rate-limit	protocol, port and destination
SSDP amplification	discard	protocol, port 1900, source any
SNMP amplification	discard	protocol, port, destination

Note: SSDP - *Simple Service Discovery Protocol* (see draft-cai-ssdp-v1–03 does not belong on a WAN an anyway? It's used for UPnP discovery. The same goes for TCP / UDP port 1 - 19.

SNMP does to my best understanding not pass the boundaries of a company network, even not protocol version 3. And sacrificing monitoring data for the sake of the network is fine with me.